(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平１０－３２５６７

(43)公開日　平成１０年（１９９８）２月３日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
H04L 9/08			H04L 9/00	601 B	
H04H 1/00			H04H 1/00	F	
H04L 9/14			H04L 9/00	601 E	
H04N 7/167				641	
			H04N 7/167	Z	

審査請求　未請求　請求項の数３　ＯＬ　（全１１頁）

(21)出願番号　特願平８－１８９６３６

(22)出願日　平成８年（１９９６）７月１８日

(71)出願人　０００００６０１３
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　秋田　康貴
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

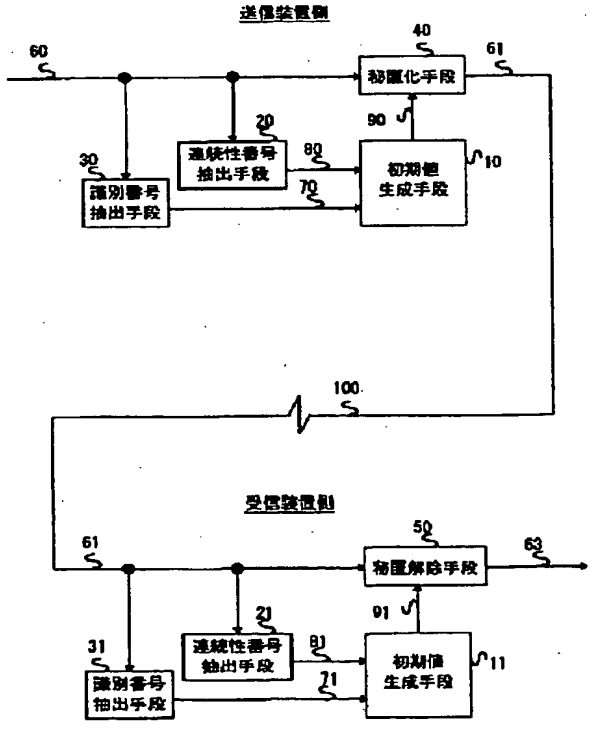
(74)代理人　弁理士　宮田　金雄　（外３名）

(54)【発明の名称】秘匿化装置、秘匿解除装置およびこれらを用いたデータ伝送システム

(57)【要約】

【課題】　送信装置と受信装置間で、メディアデータを秘匿化して送信するシステムで第３者に視聴されない秘匿強度の高いシステムを得る。

【解決手段】　送信装置においては、連続性番号抽出手段20、識別番号抽出手30でパケット60のヘッダ領域からメディアデータ連続性番号、識別番号の特定情報を抽出し、これらにより初期値生成手段10で初期値を生成し、この初期値により秘匿化手段40で送信パケット60の情報領域を秘匿化する。受信側装置は、受信パケット61のヘッダ領域から連続性番号と識別番号を連続性番号抽出手段21、識別番号抽出手段31で抽出する。これらにより初期値生成手段11で初期値を生成し、この初期値により秘匿解除手段50で受信パケットの秘匿化された情報領域の秘匿解除を行なう。



1

【特許請求の範囲】

【請求項１】　ヘッダ領域と情報領域とを有するパケットの情報領域に格納されるデータを秘匿化してパケットを送信する秘匿化装置であって、

前記パケットのヘッダ領域の特定情報を抽出する抽出手段と、前記抽出された特定情報に基づいて初期値を生成する初期値生成手段と、

前記初期値生成手段により生成された初期値に基づいて予め定められたアルゴリズムにより前記パケットの情報領域のデータを秘匿化する秘匿化手段とを備えたことを特徴とする秘匿化装置。

【請求項２】　ヘッダ領域と情報領域とを有するパケットの情報領域のデータが所定のアルゴリズムで秘匿化されたパケットの秘匿解除処理を行い復元したパケットを出力する秘匿解除装置であって、

前記受信パケットのヘッダ領域の特定情報を抽出する抽出手段と、

前記抽出された特定情報に基づいて初期値を生成する初期値生成手段と、

前記初期値生成手段により生成された初期値に基づいて所定のアルゴリズムにより前記パケットの情報領域の秘匿化データの秘匿解除を行ない復元パケットを出力する秘匿解除手段、

とを備えたことを特徴とする秘匿解除装置。

【請求項３】　ヘッダ領域と情報領域を有するパケットの情報領域に格納されるデータを秘匿化して送受信するデータ通信システムであって、

送信側装置は、送信パケットのヘッダ領域の特定情報を抽出する第１の抽出手段と、前記第１の抽出手段により抽出された特定情報に基づいて送信パケットの情報領域のデータを秘匿化するための初期値を生成する第１の初期値生成手段と、前記第１の初期値生成手段により生成された初期値に基づいて前記パケットの情報領域のデータを秘匿化しパケットを送信する秘匿化手段、

とを備え、

受信側装置では、受信パケットのヘッダ領域の特定情報を抽出する第２の抽出手段と、前記第２の抽出手段により抽出された特定情報に基づいて受信パケットの情報領域の秘匿化されたデータを解除するための初期値を生成する第２の初期値生成手段と、

前記第２の初期値生成手段により生成された初期値に基づいて受信パケットの情報領域の秘匿化されたデータを解除し復元パケットを出力する解除手段とを備えたことを特徴とするデータ伝送システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、メディアデータなどの送信データをパケット化し、パケット化されたデータに秘匿化を行ったパケットを送信装置から受信装置に伝送する場合に用いられ、第三者によるデータの内容の傍受を回避するためにデータを秘匿化する秘匿化装置と秘匿化されたデータを解除する秘匿解除装置およびこれらを用いたデータ伝送システムに関するものである。

2

【０００２】

【従来の技術】近年伝送路の高帯域化や高能率圧縮符号化方式が進展してきたことにより、映像や音声等のメディアデータを効率的に伝送するデータ通信が普及してきた。企業内におけるテレビ会議システムや有料放送システム等の導入がその代表例である。一方、これらのシステムの導入が普及するにつれて第三者による社外秘情報の傍受や、非加入者による有料放送の不正視聴などの可能性も高まっている。このような事態を回避するために、特定の秘匿化アルゴリズムによりメディアデータを送信装置側で秘匿化し、受信装置側で秘匿化されたメディアデータを秘匿解除して元のメディアデータに復元することが一般的となってきている。

【０００３】メディアデータの伝送、特にリアルタイム性が要求される映像とこれに付随する音声の伝送においてデータの秘匿化を行う場合には、秘匿化すべき各メディアデータを適当な長さに区切ってブロック化し、ブロック単位で秘匿化し、秘匿化処理を開始する毎に所定の初期値を用いることにより、万一伝送路上において秘匿化ブロック内でビット誤りが発生してもその誤りが他の秘匿化ブロックに波及しないようにし、秘匿解除が不可能となるのがビット誤りの発生した特定の秘匿化ブロックだけとなるようにするのが一般的である。図９は、例えば「６４ビットのブロック暗号アルゴリズムの利用モード」（ＪＩＳ　Ｘ　５０５２、ＩＳＯ　８３７２）で示されているＣＢＣ（ＣｉｐｈｅｒＢｌｏｃｋ　Ｃｈａｉｎｉｎｇ）モードの動作を説明する図である。図中、暗号化処理部は請求項１に記載の秘匿化手段に相当する。また復号処理部は請求項２に記載の秘匿解除手段に相当する。このモードでは、暗号化処理の過程で暗号文を平文側にフィードバックする。E_iを鍵Ｋによる暗号化、D_iを鍵Ｋによる復号、C_iを初期値、P_iを平文ｉ、C_iを暗号文ｉとすると、下記の式（１）のように表わせる。

【０００４】

【数１】

$$C_i = E_k(P_i \oplus C_{i-1})$$
$$P_i = D_k(C_i) \oplus C_{i-1}$$

⊕…排他論理和

【０００５】初期値C_iは、ブロック化されたデータを暗号化処理するための最初の入力値である。鍵が同じでも初期値を変更すると同じ平文から異なる暗号文を生成することができる。従って、ブロック単位に初期値を変更すれば、暗号強度を高めることができる。

【０００６】図８は、特開昭６３－１６７５８８号公報

に示された従来の秘匿化データ伝送システムである。図において、伝送データ処理手段２１１は映像信号２１０を入力して秘匿化を行う回路であり、同処理手段２１１の出力はデータ重畳手段２１２を介して伝送路２１３に導かれる。映像信号２１０は伝送回数制御手段２１４にも供給されている。伝送回数制御手段２１４は映像信号２１０の垂直同期信号をカウントして信号２１４ａ、２１４ｂ、２１４ｃを出力している。このうち信号２１４ａは垂直同期信号がカウントされる毎にインクリメントする信号であり、初期値変換手段２１６に入力される。伝送回数制御手段２１４の出力信号２１４ｂ、２１４ｃは、初期値２１５ａを変更するタイミングを与える信号であり、例えばｎフィールド毎に初期値を変更する場合、伝送回数制御手段２１４の最大カウント値がｎに設定され、このとき信号２１４ｂはカウント値ｎに対応して出力される。これによりｎカウント値出力２１４ｂのタイミングで新たな初期値２１５ａが発生され、重畳データ作成手段２１７はｎカウント出力時に同期パターン発生手段２１８の出力を選択し、それ以外の期間に初期値２１５ａを選択する。なお初期値発生手段２１５はカウント値ｎから次カウント周期のｎ－１まで新たな初期値２１５ａを維持している。

【０００７】一方、初期値変換手段２１６は、上記の新たな初期値２１５ａが初期値発生手段２１５より発生するタイミングで以前に発生していた初期値２１５ａをｎフィールド期間ラッチ出力する機能を有しており、このラッチ出力された以前の初期値は、信号２１４ａの各インクリメント値で所定の論理変換を受け、その変換データに基づく乱数信号２１６ａを発生する。そしてこの出力する乱数信号２１６ａのタイミングで伝送データ処理手段２１１に入力した映像信号を秘匿化する。なお本従来例では映像のフィールド単位が秘匿化すべきデータのブロック単位となっていることは明らかである。

【０００８】こうして伝送路２１３には上記変換データを初期値として秘匿化された映像信号２２５が伝送される。伝送路２１３からの秘匿化映像信号２１９は、受信データ処理手段２２０、データ抽出手段２２１及び伝送回数カウント手段２２２に供給されている。受信データ処理手段２２０は送信装置側における伝送データ処理手段２１１と逆の処理を行い、秘匿化映像信号２１９を秘匿解除する回路である。また、データ抽出手段２２１は所定期間に重畳された初期値を各フィールド毎すべて抽出する回路である。伝送回数カウント手段２２２は秘匿化映像信号２１９における垂直同期信号をカウントし、そのカウント出力２２２ａを初期値変換手段２２３に供給する。この場合、伝送回数カウント手段２２２は、同期パターンを検索するする同期パターン検出手段２２４が同期パターンを検出すると、それのタイミングを示す信号２２４ａによってカウンタ値がクリアされる。これにより初期値変換手段２２３は送信装置側と同一の乱数信号２２３ａを出力することになり、受信データ処理手段２２０からは正確に秘匿解除された映像信号２２６が出力される。

【０００９】

【発明が解決しようとする課題】従来の秘匿化データ伝送システムは以上のように構成されており、ｎフィールド毎に初期値を変更し、さらに所定の論理変換を行った初期値を伝送する。しかし所定の論理変換を行っているとはいえ、伝送路上に初期値が出現するのであり、第三者によりこの初期値が解読され、伝送される秘匿化データが秘匿解除されて不正に視聴される場合があるという問題点があった。本発明は上記のような問題点を解消するためになされたもので、送信装置と受信装置間で初期値を伝送せずに秘匿化処理を実現するとともに、秘匿化すべきデータを適当な長さに区切ってブロック化、すなわちパケット化し、各パケットの秘匿化処理を開始する毎に所定の初期値を用いることにより、秘匿強度を高めた秘匿化データ伝送システムを得ることを目的とする。

【００１０】

【課題を解決するための手段】この発明の第１の発明は、ヘッダ領域と情報領域とを有するパケットの情報領域に格納されるデータを秘匿化してパケットを送信する秘匿化装置であって、前記パケットのヘッダ領域の特定情報を抽出する抽出手段と、前記抽出された特定情報に基づいて初期値を生成する初期値生成手段と、前記初期値生成手段により生成された初期値に基づいて予め定められたアルゴリズムにより前記パケットの情報領域のデータを秘匿化する秘匿化手段を備える。

【００１１】この発明の第２の発明は、ヘッダ領域と情報領域とを有するパケットの情報領域が所定のアルゴリズムで秘匿化されたパケットの秘匿解除処理を行い復元したパケットを出力する秘匿解除装置であって、前記受信パケットのヘッダ領域の特定情報を抽出する抽出手段と、前記抽出された特定情報に基づいて初期値を生成する初期値生成手段と、前記初期値生成手段により生成された初期値に基づいて所定のアルゴリズムにより前記パケットの情報領域の秘匿化データの秘匿解除を行ない復元パケットを出力する秘匿解除手段を備える。

【００１２】この発明の第３の発明は、ヘッダ領域と情報領域を有するパケットの情報領域に格納されるデータを秘匿化して送受信するデータ通信システムであって、送信側装置は、送信パケットのヘッダ領域の特定情報を抽出する第１の抽出手段と、前記第１の抽出手段により抽出された特定情報に基づいて送信パケットの情報領域のデータを秘匿化するための初期値を生成する第１の初期値生成手段と、前記第１の初期値生成手段により生成された初期値に基づいて前記パケットの情報領域のデータを秘匿化しパケットを送信する秘匿化手段、とを備え、受信側装置では、受信パケットのヘッダ領域の特定情報を抽出する第２の抽出手段と、前記第２の抽出手段

により抽出された特定情報に基づいて受信パケットの情報領域の秘匿化されたデータを解除するための初期値を生成する第２の初期値生成手段と、前記第２の初期値生成手段により生成された初期値に基づいて受信パケットの情報領域の秘匿化されたデータを解除し復元パケットを出力する解除手段を備える。

【００１３】

【発明の実施の形態】

実施の形態１．以下、本発明の一実施の形態を図について説明する。図１は、本発明に係る秘匿化データ伝送システムの一実施の形態を示す図である。図２は、本発明に係る秘匿化データ伝送システムで伝送されるパケットの構成を示す図、図３は、秘匿化前及び秘匿解除後のパケットと秘匿化パケットの構成を示す図、図４は本発明に係るパケットの秘匿化処理と秘匿解除処理のタイミングチャートを示す図、図５は本発明に係る初期値生成手段の構成を示す図、図６は本発明に係る秘匿化手段の構成を示す図、図７は本発明に係る秘匿解除手段の構成を示す図である。なお、図４で示すタイミングチャートは本発明の動作説明用のものであり、厳密なタイミングを規定するものではない。

【００１４】図１において、１０と１１は初期値生成手段、２０と２１は連続性番号抽出手段、３０と３１は識別番号抽出手段である。４０は秘匿化手段、５０は秘匿解除手段、１００は伝送路である。６０は送信パケット、６１は秘匿化パケット、６３は秘匿解除パケットで送信パケット６０と同一である。７０と７１はメディアデータなどデータの種類を識別する識別番号で、パケットの情報領域に格納されたメディアデータなどのデータの種類に応じてユニークに割り当てられた番号である。８０と８１は連続性番号で、パケットを伝送する毎に所定の順序付け方法にて順序つけられた番号である。ここで、この実施の形態では、ヘッダ領域の連続番号と識別番号を特定情報とし、連続性番号抽出手段と識別番号抽出手段をヘッダ領域の特定情報を抽出する抽出手段とする。図２において、６４はパケットのヘッダ領域、６５はパケットの情報領域である。情報領域６５にはメディアデータが格納される。ヘッダ領域６４には、上述のメディアデータ識別番号と連続性番号とが格納される。図３において、（ａ）は秘匿化前または秘匿解除後のメディアデータを情報領域に格納したパケットの構成、（ｂ）は秘匿化されたメディアデータを情報領域に格納したパケットの構成を示す。

【００１５】送信装置において、送信パケット６０が秘匿化パケット６１として出力されるまでを図１、図４、図５、図６を用いて説明する。送信パケット６０は、識別番号抽出手段３０、連続性番号抽出手段２０及び秘匿化手段４０に供給されており、その構成は図２に示す通りである。識別番号抽出手段３０は、メディアデータを情報領域に格納した送信パケット６０を入力し、当該パケットのヘッダ領域を検出し、当該メディアデータを識別するためにユニークに割り当てられたメディアデータ識別番号７０をそのヘッダ領域から抽出して初期値生成手段１０へ出力する。このとき識別番号抽出手段３０は、図４の（ａ）に示すようにメディアデータ識別番号７０を検出したら直ちに初期値生成手段１０へ出力し、少なくとも送信パケット６０の情報領域６５が入力されるまで出力保持する機能を有する。

【００１６】連続性番号抽出手段２０は、識別番号抽出手段３０に入力されるパケットと同一のパケット６０を入力し、当該パケットのヘッダ領域を検出し、伝送されるパケットの連続性を示す連続性番号８０をそのヘッダ領域から抽出して初期値生成手段１０へ出力する。このとき連続性番号抽出手段２０は、図４の（ａ）に示すように連続性番号８０を検出したら直ちに初期値生成手段１０へ出力し、少なくとも送信パケット６０の情報領域６５が入力されるまで出力保持する機能を有する。初期値生成手段１０は、送信するパケットのメディアデータ識別番号７０と連続性番号８０とをそれぞれ識別番号抽出手段３０と連続性番号抽出手段２０とから入力し、これらのメディアデータ識別番号７０と連続性番号８０との組合わせを元にして当該パケットの情報領域に格納されるメディアデータを秘匿化するために必要な初期値９０を生成して秘匿化手段４０へ出力する。このとき初期値生成手段１０は、図４の（ａ）に示すようにメディアデータ識別番号７０と連続性番号８０の両方が共に入力された時点で直ちに初期値９０を生成して秘匿化手段４０へ出力し、少なくとも送信パケット６０の情報領域６５が入力されるまで出力保持する機能を有する。

【００１７】初期値生成手段１０の構成例を図５に示す。メディアデータ識別番号７０と連続性番号８０は、次の入力があるまでそれぞれレジスタ１１１とレジスタ１１２に保持される。演算部１１３においては、レジスタ１１１とレジスタ１１２に保持されたメディアデータ識別番号７０と連続性番号８０とを入力して所定の方法で演算を実施し、複数の初期値（図中、Ｃ０１～Ｃ０ｋ）が格納されたメモリ１１４の特定のアドレスを生成する。このとき演算部１１３は、入力されるメディアデータ識別番号７０と連続性番号８０とに基づいて、加算、減算、乗算、除算のいずれかを使用した演算を実施する。メモリ１１４は、演算部１１３から与えられたアドレスに対応した初期値をその格納領域から読み出し、初期値９０として出力する。

【００１８】秘匿化手段４０は、送信パケット６０に対応した初期値９０を初期値生成手段１０から入力し、当該パケットの情報領域に格納されたメディアデータを秘匿化して秘匿化パケット６１として出力する。このとき秘匿化手段４０は、図４の（ａ）に示すように当該パケット６０の情報領域６５のメディアデータが入力される直前に初期値９０をロードし、図９に示すような秘匿化

処理を情報領域６５の最後のデータまで継続して実施する。なお、秘匿化手段４０はヘッダ領域については秘匿化を行わないので、図３の（ｂ）に示すように出力される秘匿化パケット６１は秘匿化されないヘッダ領域と秘匿化された情報領域を持つ構成となる。

【００１９】秘匿化手段４０の構成例を図６に示す。ヘッダ分離部４０１は、入力された送信パケット６０からヘッダ領域６４と情報領域６５とを分離して、それぞれヘッダレジスタ４０３と秘匿化処理部４０２に出力する。秘匿化処理部４０２は、情報領域６５に対し、与えられた初期値９０を用いて秘匿化処理を実施する。ヘッダレジスタ４０３は、分離されたヘッダ領域６４を一時的に保持する。ヘッダ付加部４０４は、秘匿化処理部４０２にて秘匿化処理が実施された情報領域６５に対して、ヘッダレジスタ４０３にて一時的に保持されたヘッダ領域６４を付加して、秘匿化パケット６１として出力する。以上のようにして伝送路１００には、情報領域が秘匿化された秘匿化パケット６１が伝送される。

【００２０】受信装置において、秘匿化パケット６１が秘匿解除されたパケット６３として出力されるまでを図１、図４、図５、図７を用いて説明する。伝送路１００から入力する秘匿化パケット６１は、識別番号抽出手段３１、連続性番号抽出手段２１及び秘匿解除手段５０に供給されており、その構成は図２に示す通りである。識別番号抽出手段３１は、秘匿化パケット６１を入力し、当該パケットのヘッダ領域を検出し、当該メディアデータを識別するためにユニークに割り当てられたメディアデータ識別番号７１をそのヘッダ領域から抽出して初期値生成手段１１へ出力する。このとき識別番号抽出手段３１は、図４の（ｂ）に示すようにメディアデータ識別番号７１を検出したら直ちに初期値生成手段１１へ出力し、少なくとも秘匿化パケット６１の情報領域６５が入力されるまで出力保持する機能を有する。

【００２１】連続性番号抽出手段２１は、識別番号抽出手段３１に入力されるパケットと同一のパケット６１を入力し、当該パケットのヘッダ領域を検出し、伝送されるパケットの連続性を示す連続性番号８１をそのヘッダ領域から抽出して初期値生成手段１１へ出力する。このとき連続性番号抽出手段２１は、図４の（ｂ）に示すように連続性番号８１を検出したら直ちに初期値生成手段１１へ出力し、少なくとも秘匿化パケット６１の情報領域６５が入力されるまで出力保持する機能を有する。初期値生成手段１１は、受信した秘匿化パケット６１のメディアデータ識別番号７１と連続性番号８１とをそれぞれ識別番号抽出手段３１と連続性番号抽出手段２１とから入力し、これらのメディアデータ識別番号７１と連続性番号８１との組合わせを元にして当該パケットの情報領域に格納されるメディアデータを秘匿解除するために必要な初期値９１を生成して秘匿解除手段５０へ出力する。このとき初期値生成手段１１は、図４の（ｂ）に示すようにメディアデータ識別番号７１と連続性番号８１の両方が共に入力された時点で直ちに初期値９１を生成して秘匿解除手段５０へ出力し、少なくとも秘匿化パケット６１の情報領域６５が入力されるまで出力保持する機能を有する。初期値生成手段１１の構成例は初期値生成手段１０の構成例を示す図５と同様であり、その動作も同様であるので、説明は省略する。

【００２２】秘匿解除手段５０は、受信した秘匿化パケット６１に対応した初期値９１を初期値生成手段１１から入力し、当該パケットの情報領域に格納されたメディアデータを秘匿解除して元のパケット６３に復元し、これを出力する。このとき秘匿解除手段５０は、図４の（ｂ）に示すように当該パケット６１の情報領域６５のメディアデータが入力される直前に初期値９１をロードし、図９に示すような秘匿処理を情報領域６５の最後のデータまで継続して実施する。秘匿解除手段５０の構成例を図７に示す。ヘッダ分離部５０１は、入力された秘匿化パケット６１からヘッダ領域６４と秘匿化された情報領域６５とを分離して、それぞれヘッダレジスタ５０３と秘匿解除処理部５０２に出力する。秘匿解除処理部５０２は、秘匿化された情報領域６５に対し、与えられた初期値９１を用いて秘匿解除処理を実施する。ヘッダレジスタ５０３は、分離されたヘッダ領域６４を一時的に保持する。ヘッダ付加部５０４は、秘匿解除処理部５０２にて秘匿解除処理が実施された情報領域６５に対して、ヘッダレジスタ５０３にて一時的に保持されたヘッダ領域６４を付加して、秘匿解除パケット６３として出力する。

【００２３】パケットの構成を示す図２についてさらに説明する。ヘッダ領域６４は当該パケットの制御情報が格納される領域であり、制御情報の中には少なくともメディアデータ識別番号と連続性番号とが格納されている。情報領域６５は、適当なデータ長に区切られたメディアデータが格納される領域である。なおひとつのパケットにおける情報領域に格納されるメディアデータは１種類である。メディアデータ識別番号は、送信装置側で付与され、情報領域６５に格納されたメディアデータの種類に応じてユニークに割り当てられた識別番号であって、受信装置はこのメディアデータ識別番号を検出して当該パケットに格納されたメディアデータの種類を判断する。連続性番号は、送信装置側で付与され、パケットを伝送する毎に所定の順序付け方法にて順序付けられた番号であって、受信装置はこの連続性番号の連続性を監視することによって受信したパケットの損失の有無等を判断する。従ってメディアデータ識別番号と連続性番号は本来上述の処理を目的としたものであり、秘匿化処理のための情報ではないのであり、メディアデータ識別番号と連続性番号とを秘匿化処理及び秘匿解除処理に利用することが本発明の特徴である。

【００２４】図３の（ａ）は送信パケット６０と秘匿解

9

除されたパケット６３（即ち元の送信パケット６０）の構成を示し、（ｂ）は秘匿化パケット６１の構成を示している。（ａ）の構成の送信パケット６０の情報領域のメディアデータが秘匿化手段４０で秘匿化されると、（ｂ）の構成の秘匿化パケット６１になる。このとき秘匿化処理の対象はパケットの情報領域だけであり、ヘッダ領域は秘匿化されない。一方、（ｂ）の構成の秘匿化パケット６１の情報領域のメディアデータは秘匿解除手段５０で秘匿解除され、（ａ）の構成のパケット６３となり、元の送信パケット６０に復元される。

【００２５】

【発明の効果】以上のように本発明による秘匿化装置、秘匿解除装置およびこれらを用いたデータ伝送システムでは、送信装置と受信装置間で伝送路を経由して初期値を伝送しないので、第三者により初期値を傍受されることがなく、従って伝送される秘匿化データが第三者により秘匿解除されて不正視聴されることを防止することができる効果がある。また各パケットの秘匿化処理を開始する毎に所定の初期値を用いる構成としたので、秘匿強度をより一層高めることができる効果がある。

【図面の簡単な説明】

【図１】　本発明に係る秘匿化データ伝送システムの構成を示す図である。

【図２】　本発明に係る秘匿化データ伝送システムで伝送されるパケットの構成を示す図である。

【図３】　本発明に係る秘匿化データ伝送システムにおける秘匿化前及び秘匿解除後のパケットと秘匿化パケットの構成を示す図である。

10

【図４】　本発明に係る秘匿化データ伝送システムにおけるパケットの秘匿化処理と秘匿解除処理のタイミングチャートを示す図である。

【図５】　本発明に係る秘匿化データ伝送システムにおける初期値生成手段の構成を説明するための図である。

【図６】　本発明に係る秘匿化データ伝送システムにおける秘匿化手段の構成を説明するための図である。

【図７】　本発明に係る秘匿化データ伝送システムにおける秘匿解除手段の構成を説明するための図である。

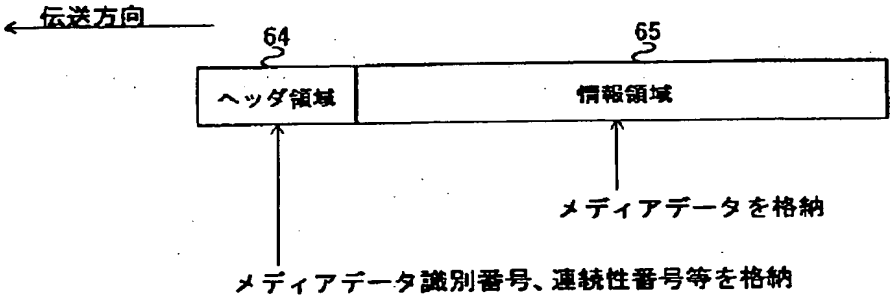
【図８】　従来の秘匿化データ伝送システムの構成を示す図である。

【図９】　「６４ビットのブロック暗号アルゴリズムの利用モード」（ＪＩＳ　Ｘ　５０５２、ＩＳＯ　８３７２）で示されているＣＢＣ（ＣｉｐｈｅｒＢｌｏｃｋ　Ｃｈａｉｎｉｎｇ）モードの動作を説明する図である。

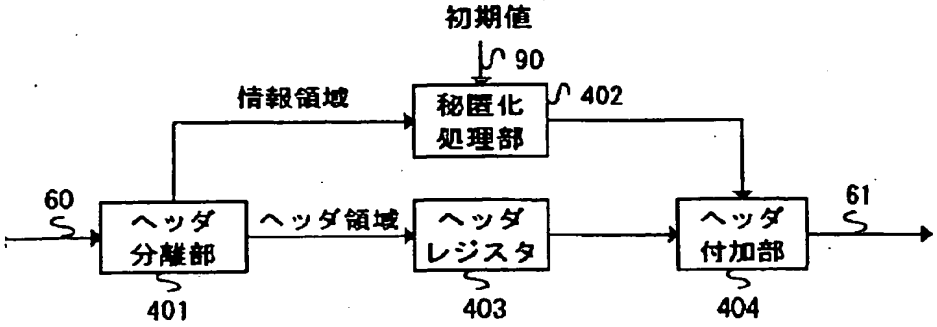
【符号の説明】

１０、１１　初期値生成手段、　２０、２１　連続性番号抽出手段、　３０、３１　識別番号抽出手段、　４０　秘匿化手段、　５０　秘匿解除手段、　６０送信パケット、　６１　秘匿化パケット、　６３　秘匿解除パケット、　６４ヘッダ領域、　６５　情報領域、　７０、７１　メディアデータ識別番号、８０、８１　連続性番号、　９０、９１　初期値、　１００　伝送路。

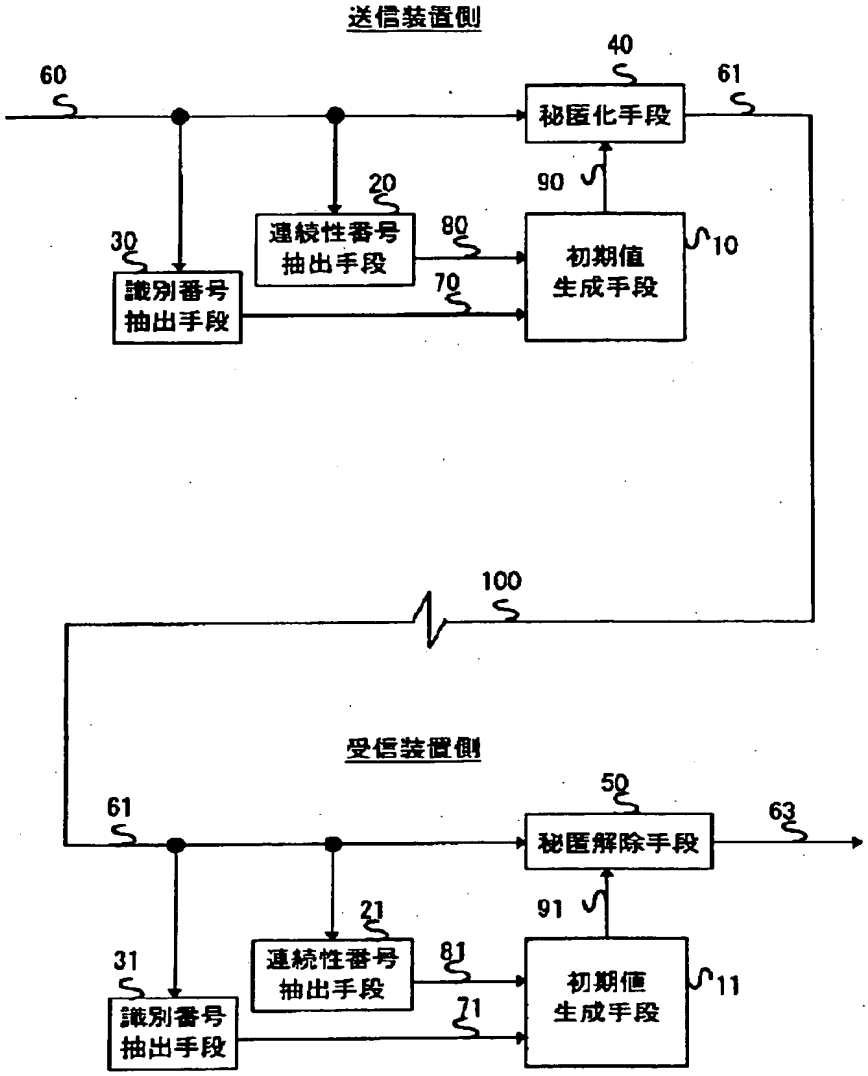
【図２】



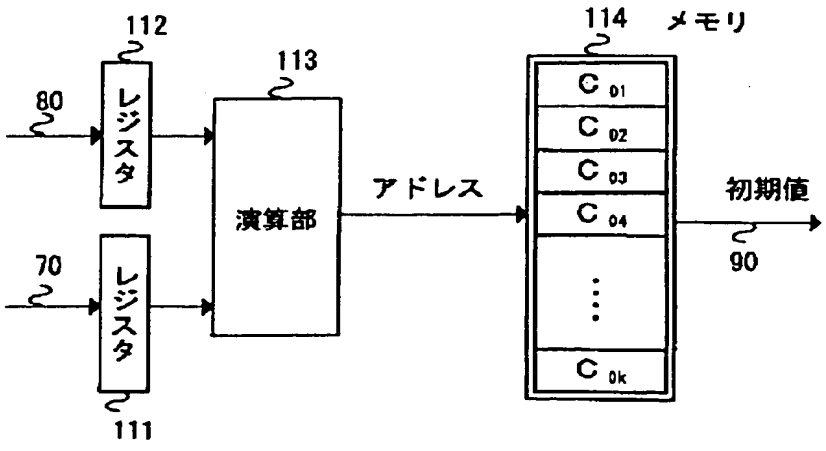
【図６】



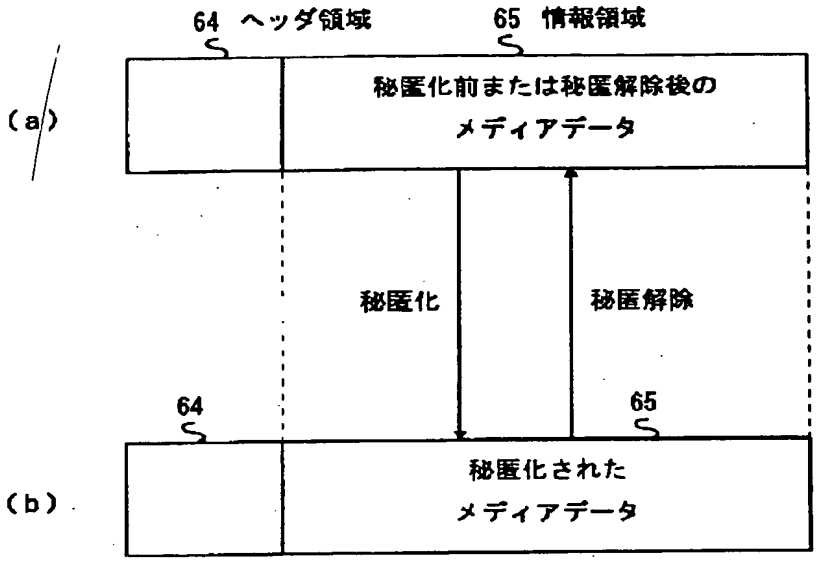
【図１】


送信装置側
60
40
秘匿化手段
61
90
20
連続性番号
抽出手段
80
初期値
生成手段
10
30
識別番号
抽出手段
70
100
受信装置側
61
50
秘匿解除手段
63
91
21
連続性番号
抽出手段
81
初期値
生成手段
11
31
識別番号
抽出手段
71

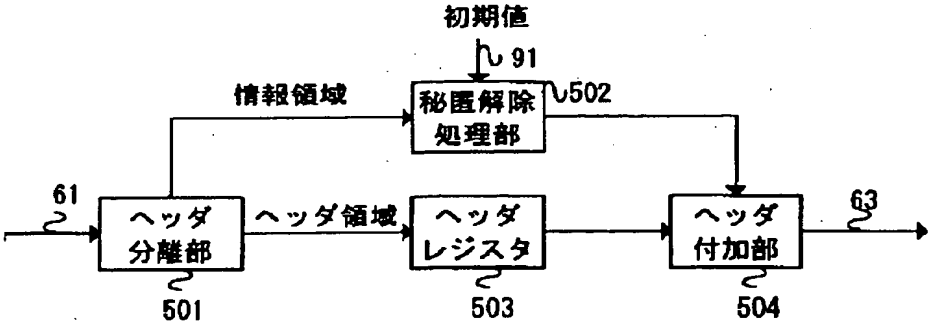
【図５】


112
113
114　メモリ
80
レジスタ
演算部
アドレス
C 01
C 02
C 03
C 04
C 0k
初期値
90
70
レジスタ
111

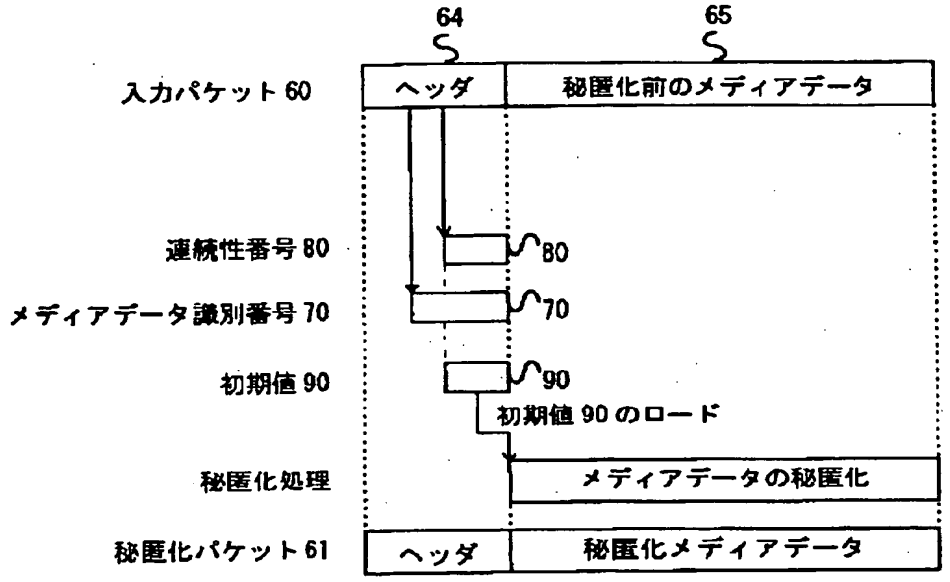
【図３】


64 ヘッダ領域
65 情報領域
(a)
秘匿化前または秘匿解除後の
メディアデータ
秘匿化
秘匿解除
64
65
秘匿化された
メディアデータ
(b)

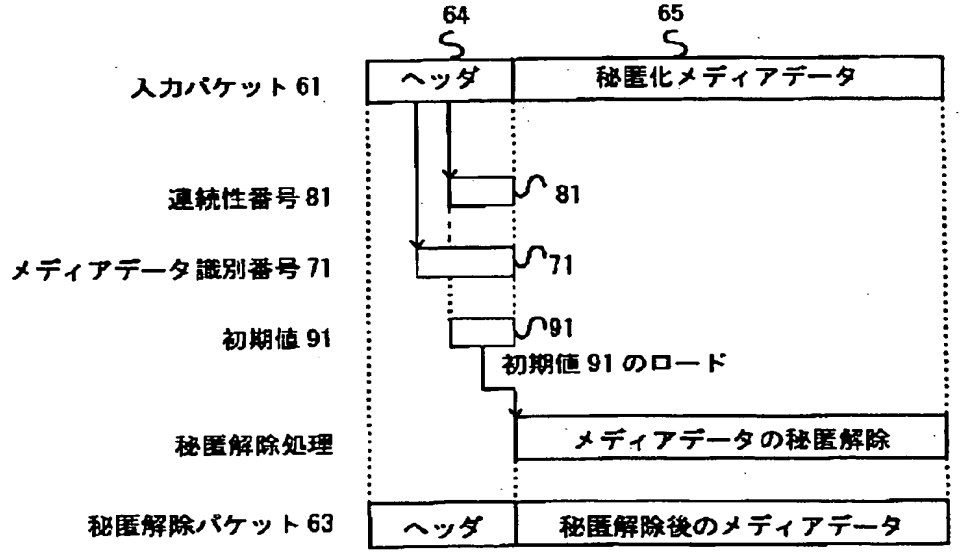
【図７】


初期値
91
情報領域
秘匿解除
処理部
502
61
ヘッダ
分離部
ヘッダ領域
ヘッダ
レジスタ
ヘッダ
付加部
63
501
503
504

【図４】

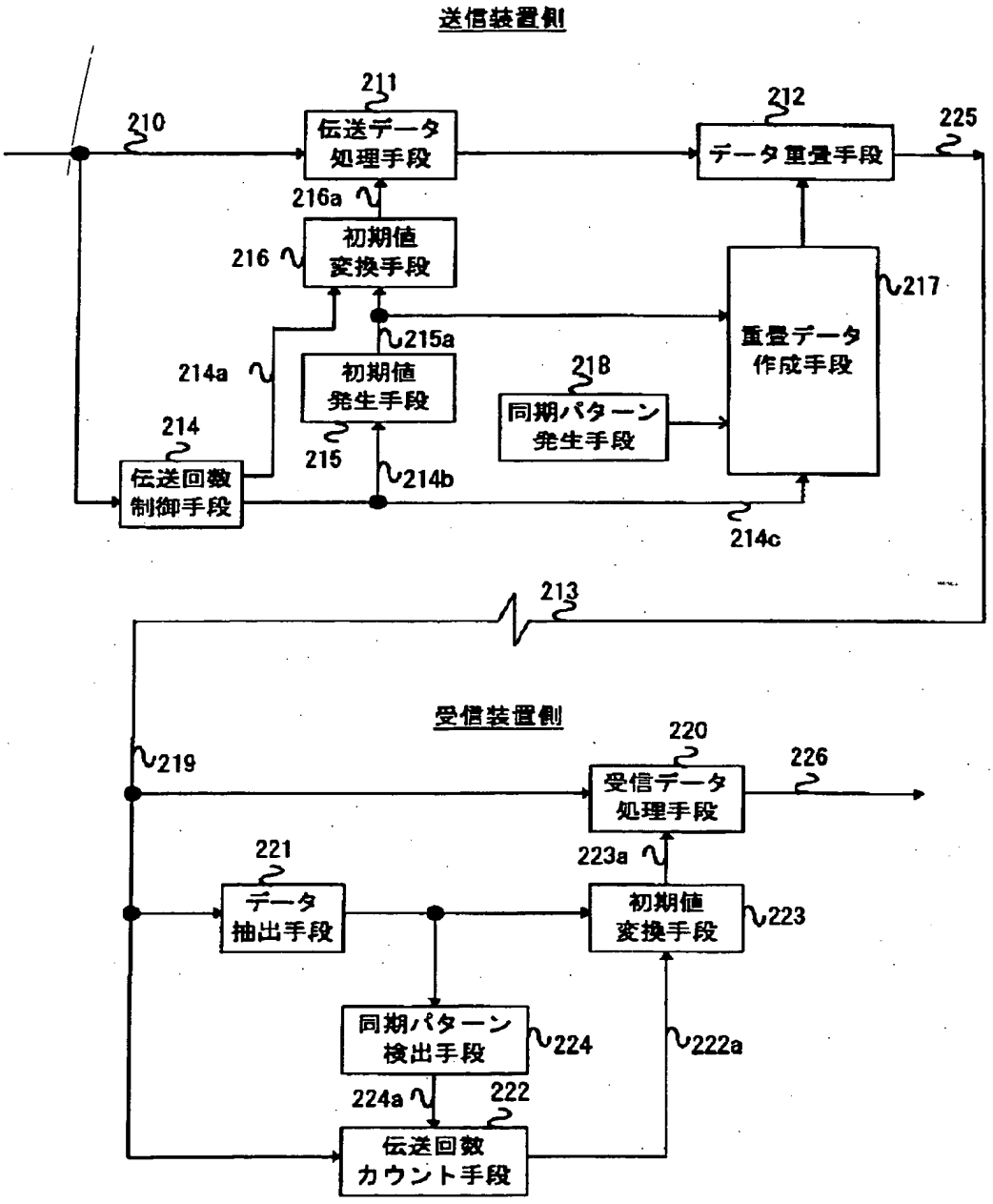


（ａ）送信装置側におけるパケットの秘匿化処理タイミング

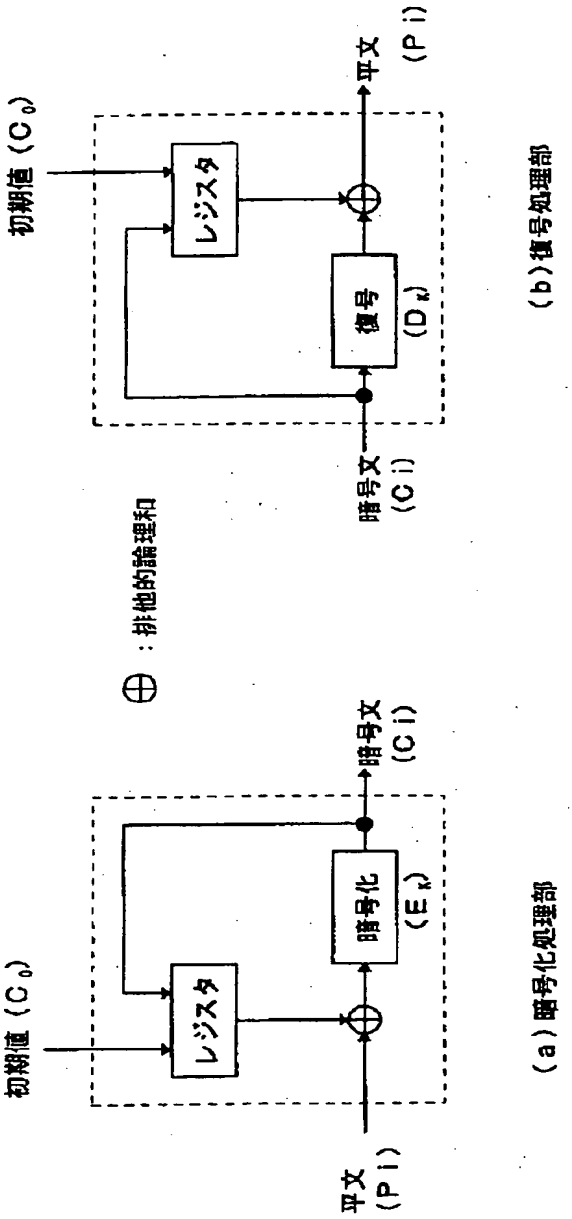


（ｂ）受信装置側におけるパケットの秘匿解除処理タイミング

【図８】


送信装置側
211
伝送データ処理手段
210
212
データ重畳手段
225
216a
初期値変換手段
216
217
重畳データ作成手段
215a
214a
初期値発生手段
218
同期パターン発生手段
214
215
伝送回数制御手段
214b
214c
213
受信装置側
219
220
受信データ処理手段
226
221
223a
データ抽出手段
初期値変換手段
223
同期パターン検出手段
224
222a
224a
222
伝送回数カウント手段

【図９】



(a) 暗号化処理部　　(b) 復号処理部